CLAIMS

1. A computer-implemented method of implementing security for SOAP messages which can be exchanged between client and server programs, the method comprising:

receiving a SOAP message;

determining whether at least one security rule is associated with the SOAP message, the at least one security rule being associated with a security policy for SOAP messages which can be exchanged between at least one client program and at least one server program; and

performing at least one operation based on the at least one security rule when the determining determines that at least one security rule is associated with the SOAP message.

2. A method as recited in claim 1, wherein the at least one security rule describes a mapping between one or more keys respectively used by the at least one client program and the at least one server program.

3. A method as recited in claim 1, wherein the performing of at least one operation maps one or more security identifiers which are recognized by the at least one client program to one or more security identifiers which are recognized by the server program.

4. A method as recited in claim 1, wherein the security identifiers can include one or more encryption keys, one or more decryption keys, one or more signing keys, and one or more keys used to verify one or more signatures.

5. A method as recited in claim 1,

wherein the method further comprises:

determining a message type for the SOAP message, and

wherein the determining of whether at least one security rule is associated with the SOAP message comprises:

looking up rules which are associated with the message type.

6. A method as recited in claim 1,

wherein the at least one security rule includes at least one decryption rule, and

wherein the performing of the at least one operation comprises:

determining whether the SOAP message is encrypted, and

decrypting the SOAP message based on one or more decryption keys which are associated with the at least one decryption rule.

7. A method as recited in claim 6, wherein the one or more decryption keys are managed by an organization or define an organizational rule.

8. A method as recited in claim 1,

wherein the at least one security rule includes at least one encryption rule, and

wherein the performing of at least one operation comprises:

encrypting the SOAP message based on one or more encryption keys which are associated with the at least one encryption rule.

9. A method as recited in claim 8, wherein the one or more encryption keys are associated with an individual.

10. A method as recited in claim 8, wherein the method further comprises:

determining whether the SOAP message is encrypted before attempting to decrypt the SOAP message.

11. A method as recited in claim 6, wherein the method further comprises:

determining whether the SOAP message has been encrypted successfully; and

taking appropriate action when the determining determines that the SOAP message has not been encrypted successfully.

12. A method as recited in claim 1,

wherein the at least one security rule includes at least one signature verification rule; and

wherein the performing of at least one operation comprises:

verifying at least one signature associated with the SOAP message per requirements specified by the at least one signature verification rule.

13. A method as recited in claim 12, wherein the method further comprises:

determining whether the at least one signature associated with the SOAP message has successfully been verified; and

taking appropriate action when the determining determines that one or more of the at least one signature has not been successfully verified.

14. A method as recited in claim 1,

wherein the at least one security rule includes a signing rule; and

wherein the performing of at least one operation comprises:

signing the SOAP message using one or more keys which are associated with the at least one security rule.

15. A method as recited in claim 1, wherein at least one portion of the SOAP message is in XML.

16. A computer-implemented method of implementing security for SOAP messages exchanged between client and server programs, the method comprising:

receiving a SOAP message;

determining whether at least one decryption rule is associated with the SOAP message;

attempting to decrypt the SOAP message using one or more keys associated with the at least one decryption rule when the determining determines that at least one decryption rule is associated with the SOAP message;

determining whether at least one encryption rule is associated with the SOAP message;

encrypting the SOAP message using one or more keys associated with the at least one decryption rule when the determining determines that at least one encryption rule is associated with the SOAP message;

determining whether at least one signature verification rule is associated with the SOAP message;

verifying at least one signature associated with the SOAP message per requirements specified by the at least one signature verification rule when the determining determines that at least one signature verification rule is associated with the SOAP message;

determining whether at least one signing rule is associated with the SOAP message; and

signing the SOAP message using one or more keys associated with the at least one signing rule.

17. A computer readable medium having computer program instructions stored therein for performing the method of claim 16.

18. A method as recited in claim 16, wherein the method further comprises:

determining a message type for the SOAP message, and

looking up rules which are associated with the message type.

19. A method as recited in claim 16, wherein at least one portion of the SOAP message is XML.

20. A method as recited in claim 16, wherein the method further comprises:

determining whether the SOAP message is encrypted before attempting to decrypt the SOAP message;

determining whether the SOAP message has been encrypted successfully; and

taking appropriate action when the determining determines that the SOAP message has not been encrypted successfully.

21. A method as recited in claim 16, wherein the method further comprises:

determining whether the at least one signature associated with the SOAP message has successfully been verified; and

taking appropriate action when the determining determines that the at least one signature has not been successfully verified.

22. A computer readable medium having computer program instructions stored therein for performing the method of claim 1.

23. A traffic manager for facilitating communication between a client node and a server node in a distributed computing environment, the server node having a first interface associated therewith which is incompatible with direct communications generated by the client node, the traffic manager comprising a central processing unit which can operate to:

receive a SOAP message;

determine whether at least one security rule is associated with the SOAP message, the at least one security rule being associated with a security policy for SOAP messages which can be exchanged between at least one client program and at least one server program; and

perform at least one operation based on the at least one security rule when the determining determines that at least one security rule is associated with the SOAP message.

24. A traffic manager as recited in claim 23, wherein the at least one security rule describes a mapping between one or more keys respectively used by the at least one client program and the at least one server program.

25. A traffic manager as recited in claim 23, wherein the performing of at least one operation maps one or more security identifiers which are recognized by the at least one client program to one or more security identifiers which are recognized by the server program.

26. A method as recited in claim 25, wherein the one or more security identifiers can include one or more encryption keys, one or more decryption keys, one or more signing keys, and one or more keys used to verify one or more signatures.

27. A computer-implemented method of protecting a server program from service attacks, the method comprising:

receiving a SOAP message;

determining whether at least one rule is associated with the SOAP message;

collecting data that may be required to evaluate the at least one rule;

evaluating the at least one rule at least partially based on the collected data; and

determining whether the SOAP message constitutes a service attack based on the evaluating of the at least one rule.

28. A method as recited in claim 27, wherein the determining of whether at least one rule is associated with the SOAP message comprises at least one of the acts of:

(a) determining a message type for the SOAP message;

(b) determining a sender node for the SOAP message; and

(c) determining a recipient node for the SOAP message.

29. A method as recited in claim 28, wherein the determining of data that may be required to evaluate the at least one rule comprises:

determining which portion of history of at least one of the message type, sender node, and recipient node should be collected.

30. A method as recited in claim 27, wherein the method further comprises:

denying service when the determining determines that the SOAP message constitutes a service attack.

31. A method as recited in claim 30, wherein the method further comprises:

taking remedial action when the determining determines that the SOAP message constitutes a service attack.

32. A method as recited in claim 30, wherein the one or more remedial actions include notifying an administrator, holding the SOAP message, making a log entry, invoking a programming object, and sending an additional SOAP message.

33. A computer-implemented method of protecting a server program from service attacks, the method comprising:

receiving a SOAP message;

determining at least one of: (a) a message type for the SOAP message, (b) a sender for the SOAP message, and (c) a recipient for the SOAP message;

determining whether at least one rule is associated with at least one of the message type (a) , the sender (b), and the recipient (c);

selecting at least one portion of the data which has been collected for at least one of the message type (a) , the sender (b), and the recipient (c);

evaluating the at least one rule using the selected at least one portion of data; and

determining whether the SOAP message constitutes a service attack based on the evaluating of the at least one rule.

34. A method as recited in claim 27, wherein the method further comprises:

denying service when the determining determines that the SOAP message constitutes a service attack.

35. A method as recited in claim 33, wherein the method further comprises:

taking remedial action when the determining determines that the SOAP message constitutes a service attack.

36. A method as recited in claim 7, wherein the remedial action includes notifying an administrator, holding the SOAP message, making a log entry, invoking a programming object, and sending an additional SOAP message.

37. A computer readable medium having computer program instructions stored therein for performing the method of claim 27.

38. A traffic manager for facilitating communication between a client node and a server node in a distributed computing environment, the server node having a first interface associated therewith which is incompatible with direct communications generated by the client node, the traffic manager comprising a central processing unit which can operate to:

receive a SOAP message;

determine whether at least one rule is associated with the SOAP message;

collect data that may be required to evaluate the at least one rule;

evaluate the at least one rule at least partially based on the collected data; and

determine whether the SOAP message constitutes a service attack based on the evaluating of the at least one rule.

39. A computer-implemented method of controlling publication of or access to a SOAP interface associated with one or more server programs, the method comprising:

identifying a SOAP interface for which publication or access is requested;

determining whether one or more rules are associated with the SOAP interface, the one or more rules describing one or more policies with respect to publication of or access to the SOAP interface;

evaluating the SOAP interface; and

determining whether publication of or access to the SOAP interface should be granted based on the evaluating of the SOAP interface.

40. A method as recited in claim 39, wherein the method further comprises:

identifying a WSDL file for the SOAP interface.

41. A method as recited in claim 40, wherein a programmer identifies the SOAP interface and the WSDL file.

42. A method as recited in claim 41, wherein the programmer interacts with a user interface to identify the SOAP interface and the WSDL file.

43. A method as recited in claim 42,

wherein the programmer interacts with a user interface of a traffic manager to determine whether one or more existing rules are associated with the SOAP interface; and

wherein the programmer interacts with a user interface of a traffic manager to request that one or more rules be approved for the SOAP interface.

44. A method as recited in claim 42, wherein the one or more rules associated with the SOAP interface can be rules associated with at least one of: a message type, a sender, or a recipient of SOAP messages that can be passed through the SOAP interface.

45. A method as recited in claim 39, wherein the evaluating of the SOAP interface is done at least partly based on one or more rules associated with the SOAP interface.

46. A method as recited in claim 45, wherein the evaluating of the SOAP interface is done at least partly by a person.

47. A method as recited in claim 46, wherein the person is an administrator.

48. A method as recited in claim 47, wherein the method further comprises:

modifying the SOAP interface.

49. A method as recited in claim 48, wherein the modifying is performed at least partly by a person.

50. A method as recited in claim 49, wherein the person is an administrator.

51. A computer readable medium having computer program instructions stored therein for performing the method of claim 39.

52. A traffic manager for facilitating communication between a client node and a server node in a distributed computing environment, the server node having a first interface associated therewith which is incompatible with direct communications generated by the client node, the traffic manager comprising a central processing unit which can operate to:

identify a SOAP interface for which publication or access is requested;

determine whether one or more rules are associated with the SOAP interface, the one or more rules describing one or more policies with respect to publication of or access to the SOAP interface;

evaluate the SOAP interface; and

determine whether publication of or access to the SOAP interface should be granted based on the evaluating of the SOAP interface.

53. A computer-implemented method of controlling publication of or access to a SOAP interface to one or more server programs, the method comprising:

(a) identifying a SOAP interface and a WSDL file for the SOAP interface for which publication or access is requested; wherein the identifying can be performed by a first person by accessing a user interface of a SOAP traffic manager;

(b) determining whether one or more rules already apply to the SOAP message, the one or more rules describing one or more policies with respect to publication of or access to the SOAP interface; wherein the determining (b) can be performed by the first person by accessing a user interface to a SOAP traffic manager;

(c) requesting approval of one or more additional rules for the SOAP message wherein the requesting can be performed by the first person by accessing a user interface to a SOAP traffic manager;

(d) evaluating the SOAP interface or at least one rule associated with the SOAP interface, wherein the evaluating can be performed at least partly by a second person who can access the SOAP traffic manager, and wherein the at least one rule can be a pre-existing rule or an additional rule; and

(e) determining whether the SOAP interface or at least one rule associated with the SOAP interface should be approved at least partly based on the evaluating; wherein the determining (e) can be performed at least partly by a second person who can access the SOAP traffic manager.

54. A method as recited in claim 39, wherein the first person is a programmer and the second person is an administrator.

55. A method as recited in claim 39, wherein the method further comprises:

modifying the SOAP interface or one or more additional rules for the SOAP interface, wherein the modifying can be performed at least partly by a second person who can access the SOAP traffic manager.

56. A computer-implemented method of processing SOAP messages, the method comprising:

receiving a SOAP message;

determining whether at least one rule is associated with the SOAP message;

evaluating the at least one rule based on at least one portion of the SOAP message; and

determining whether an action should be taken with respect to the SOAP message based on the evaluating of the at least one rule.

57. A method as recited in claim 56, wherein the method further comprises:

determining whether at least a portion of data of the SOAP message should be considered to evaluate the at least one rule when the determining determines that at least one rule is associated with the SOAP message.

58. A method as recited in claim 56, wherein the determining of whether at least one rule is associated with the SOAP message comprises at least the acts of:

(a) determining a message type for the SOAP message;

(b) determining a sender node for the SOAP message; and

(c) determining a recipient node for the SOAP message.

59. A method as recited in claim 56, wherein the at least one rule specifies at least a portion of the SOAP message which needs to be considered to evaluate the at least one rule.

60. A method as recited in claim 59, wherein the method further comprises:

gathering at least one portion of the SOAP message.

61. A method as recited in claim 56, wherein the method further comprises:

taking one or more actions when the determining of whether an action is required determines that action is required.

62. A method as recited in claim 56,

wherein the method further comprises:

taking one or more actions when the determining of whether an action is required determines that action is required, and

wherein the one or more actions include: holding the SOAP message, archiving the SOAP message, failing SOAP message delivery, sending a notification, and logging special notification.

63. A method as recited in claim 62, wherein the SOAP message is held for review by a person.

64. A computer readable medium having computer program instructions stored therein for performing the method of claim 56.

65. A traffic manager for facilitating communication between a client node and a server node in a distributed computing environment, the server node having a first interface associated therewith which is incompatible with direct communications generated by the client node, the traffic manager comprising a central processing unit which can operate to:

receive a SOAP message;

determine whether at least one rule is associated with the SOAP message;

evaluate the at least one rule based on at least one portion of the SOAP message; and

determine whether an action should be taken with respect to the SOAP message based on the evaluating of the at least one rule.

66. A computer-implemented method of processing SOAP messages, the method comprising:

receiving a SOAP message;

determining at least one of (a) a message type for the SOAP message, (b) a sender for the SOAP message, and (c) a recipient for the SOAP message;

determining whether at least one conditional data rule is associated with at least one of the message type (a), the sender (b), and the recipient (c);

selecting at least one portion of the SOAP message based on the at least one conditional data rule;

evaluating the at least one rule using the selected at least one portion of the SOAP message; and

determining whether action is required to be taken with respect to the SOAP message based on the evaluating.

67. A method as recited in claim 66, wherein the method further comprises:

taking one or more actions when the determining of whether an action is required determines that action is required.

68. A method as recited in claim 67,

wherein the method further comprises:

taking one or more actions when the determining of whether an action is required determines that action is required, and

wherein the one or more actions include: holding the SOAP message, archiving the SOAP message, failing SOAP message delivery, sending a notification, and logging special notification.